

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched**or identify the person by name and address)*

Nokia cell phone, model N139DL, bearing IMEI number
358712914117294, obtained from William Kisor now held in
the FCSO ICAC property room at 410 S. High Street,
Columbus, Ohio 43215

Case No. 2:23-mj-513

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 U.S.C. 2252 and 2252A
 18 U.S.C. 2422(b)

Offense Description
 Receipt, distribution, and possession of Child Pornography
 Attempted coercion or enticement of a minor to engage in illegal sexual activity

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Joseph Smith
 Applicant's signature

HSI TFO Joseph Smith
 Printed name and title

Sworn to before me and signed in my presence.

Date: 9/14/2023

City and state: Columbus, Ohio

Chelsey M. Vascara
 Chelsey M. Vascara
 United States Magistrate Judge

Chelsey M. Vascara, U.S. Magistrate Judge
 Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

In the Matter of the Search of:

One (1) Nokia N139DL, bearing IMEI number 358712914117294, obtained from William Kisor and currently held in the FCSO ICAC property room at 410 S. High Street, Columbus, Ohio 43215

Case No. 2:23-mj-513

Magistrate: Vascura

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Joseph Smith (Your Affiant), a Task Force Officer with the Homeland Security Investigations (HSI), being duly sworn, hereby depose and state:

1. I, Task Force Officer Joseph Smith (your affiant), make this affidavit in support of a warrant to search a Nokia cellular phone belonging to William KISOR for violations of Title 18 United States Code §§ 2252, 2252A, and 2422(b) – the possession, receipt, or distribution of child pornography, and the attempted coercion or enticement of a minor. The statements contained in this affidavit are based in part on information and analysis provided by law enforcement agents; written reports about this and other investigations that I have received; and your affiant's personal knowledge and findings during the investigation. This affidavit is being submitted for the limited purpose of establishing probable cause for a search warrant for the content of the following device: one (1) Nokia N139DL bearing IMEI number 358712914117294 (hereinafter SUBJECT DEVICE). Your affiant did not withhold any information or evidence that would negate probable cause. Your affiant set forth only the facts that are believed to be necessary to establish probable cause to search the SUBJECT DEVICE.

2. Your affiant is a detective with the Franklin County Sheriff's Office (FCSO) Special Investigations Unit (SIU) Internet Crimes Against Children Task Force (ICAC) and has been credentialed as a Task Force Officer (TFO) with the HSI Office of the Assistant Special Agent in Charge (ASAC) in Columbus, Ohio. Your affiant has worked in SIU for approximately five years and has been a TFO with HSI since April of 2023. Your affiant has a B.S. in Security and

Intelligence and a M.B.A. in Fraud and Forensic Examination and gained experience through the completion of the HSI TFO Training Program. Your affiant has received specialized professional training in computer forensic analysis from a subsidiary of Raytheon Technologies, the International Society of Forensic Computer Examiners. Your affiant has specialized professional training in sexually and nudity-oriented matter involving children from the FCSO, HSI, ICAC, and other industry experts through formal and informal instruction. Your affiant's primary duties are and have been the investigation of violations of Titles 8, 18, 19, and 21 of the United States Code in addition to sex crimes as defined by the Ohio Revised Code. Your affiant has received specialized training and has experience in the above areas. Your affiant has completed numerous applications for criminal complaints, summonses, and search warrants.

I. PURPOSE OF THE AFFIDAVIT

3. The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for a search warrant for the contents of the SUBJECT DEVICE, which is associated with telephone number (614) 753-6570 and was seized from William R. KISOR while he was incarcerated at Alvis House, a halfway house for offender reentry. The SUBJECT DEVICE was seized on July 26, 2023, by Alvis House staff in accordance with the cellphone policy established by the Alvis House, was obtained by your affiant on or about August 29, 2023, and is currently held in the custody of the FCSO ICAC located at 410 S. High Street, Columbus, Ohio 43215.

4. The SUBJECT DEVICE to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252, 2252A, and 2422(b) – the distribution, receipt, and possession of child pornography in addition to coercion and enticement of a minor. I am requesting authority to search the entirety of the SUBJECT DEVICE, wherein the items

specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence, fruits, and instrumentalities of the above violations.

5. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, see 18 U.S.C. § 2711(3)(A)(i).

II. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess, or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

7. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

8. Title 18, United States Code, Section 2422(b) makes it a federal crime for any person to knowingly use a means of interstate commerce to persuade, induce, entice, or coerce or attempt to persuade, induce, entice, or coerce, any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person may be charged with a crime.

9. As it used in 18 U.S.C. § 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) (A) as: actual or simulated sexual intercourse, including genital-genital, oral-genital,

anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

10. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography”¹ is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

12. The term “minor”, as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as “any person under the age of eighteen years.”

13. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

the time that the sexually explicit conduct is being depicted.”

14. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”

15. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

III. BACKGROUND REGARDING DIGITAL DEVICES AND THE INTERNET

16. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files (“objects”) may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime; and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

17. Computers, mobile devices, and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

18. Computers, tablets, and smart/cellular phones (“digital devices”) are capable of storing and displaying photographs. The creation of computerized or digital photographs can be

² The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

accomplished with several methods, including using a "scanner," which is an optical device that can digitize a hard copy photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

19. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

20. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128 Gigabytes. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or

video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol (“IP”) addresses, and other information both in computer data format and in written record format.

22. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user’s true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

23. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can sometimes be recovered months or even years later using readily available forensic tools. When a person “deletes” a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

24. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

25. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

26. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law

enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

IV. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
 - b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
28. In order to fully retrieve data from a computer system or mobile computing device, the

analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored internally or on external media).

V. SEARCH METHODOLOGY TO BE EMPLOYED

29. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;
- c. Surveying various files, directories and the individual files they contain;
- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

VI. INVESTIGATION AND PROBABLE CAUSE

30. On or about January 23, 2002, KISOR was convicted by a jury in the Western District of Tennessee of one count of coercion or enticement of a juvenile in violation of 18 U.S.C. § 2422(b). In April of 2022, he was sentenced pursuant to the guilty verdict to 46 months of imprisonment, followed by three years of supervised release. While he was incarcerated on this offense, KISOR was charged by way of Information in the Southern District of Ohio with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2). Subsequent to his

guilty plea to this offense, on June 16, 2004, KISOR was sentenced to 108 months of imprisonment partially concurrent his sentence from the Western District of Kentucky case, and three years of supervised release. His term of supervised release began in October of 2011, and in July of 2012, the supervision from the Western District of Kentucky was transferred to the Southern District of Ohio.

31. In or about June of 2012, HSI in San Diego, California began an investigation of KISOR. The investigation was based on KISOR's communications on an Internet Relay Chat (IRC) and via Yahoo! chat with an undercover HSI agent. During those chats, KISOR repeatedly indicated his desire to engage in various sexually activities with the undercover's fictitious five-year-old daughter. KISOR also sent the undercover links to various images of minor children engaged in sexually explicit conduct. During the course of the investigation, it was discovered that KISOR was simultaneously chatting on IRC with an undercover HSI agent located in Denver, about engaging in sexual activities with the undercover's fictitious daughters, who were represented to be four and 14 years old at the time of the chats in 2012. The information from both undercover investigations was forwarded to law enforcement in the Southern District of Ohio, where KISOR was residing at the time.

32. As a result of the information provided by HSI San Diego and HSI Glenwood Springs, CO, HSI Columbus and the Franklin County Ohio ICAC TF executed a search warrant at KISOR residence in Circleville, Ohio. The search of KISOR's digital devices revealed the presence of Child Sexual Abuse Materials (CSAM), and KISOR was charged by way of information with possession of child pornography by a previously convicted sex offender, in violation of 18 U.S.C. § 2252(a)(4)(B).

33. In October of 2012, KISOR plead guilty to the possession of child pornography charge. In January of 2013, he was sentenced on that guilty plea to a term of 135 months of imprisonment. On the same day, he admitted that he had violated the terms of his supervised release in both the prior Western District of Tennessee an Southern District of Ohio cases. The court imposed 24-month sentences for the supervised release violations in both cases, with the sentences to run concurrently to each other, and consecutive to the sentence in the 2012 case. No new terms of supervised release were imposed on the prior cases, but the court imposed a 10-year term of supervised release in the 2012 case.

34. On or about December 28, 2022, KISOR was transitioned by the Bureau of Prisons (BOP) from federal prison to Alvis House, located at 1755 Alum Creek Drive, Columbus, Ohio 43207. KISOR signed the Alvis Cell Phone Agreement (form AH258). AH258 Section 3 states that KISOR understood his cell phone could be confiscated if program rules were violated. Section 5 states that Alvis staff or supervising authority can search KISOR's cell phone at any time with or without cause. Section 4 specified that there would be no male-to-female contact using the cell phone. Section 7 specified that KISOR was not permitted to have any nudity on his cell phone. Section 9 specified that KISOR would not use his cell phone for any illegal purposes or violation of facility rules.

35. In or about July of 2023, your affiant was informed that KISOR had contacted the HSI undercover agent from Colorado that he had been communicating with prior to his 2012 arrest and subsequent incarceration. KISOR was not previously provided any information indicating that the UC was a law enforcement officer, and his communications with the UC indicate that he still believes her to be a mother who engaged in sex acts with her minor daughters.

36. Your affiant has subsequently the chats between KISOR and the UC from 2012, as well as communications between February and June of 2023. Your affiant was also provided letters that KISOR sent to the UC while he was incarcerated. Pertinent details from those communications are described below.

37. During the 2012 communications, during which KISOR utilized IRC and the email account wrk1968@yahoo.com, KISOR stated to the UC, "yes I am a closet pefo, pedo". He also stated that he was into, "piercing, BDSM, anal, little girls, tieing up, light pain". KISOR shared CSAM when he believed he was chatting directly with the UC's fictitious then-14-year-old daughter. Throughout the course of the communications, he also sent several images of himself confirming his identity.

38. Throughout his confinement at the BOP for his 2013 child pornography conviction, KISOR solicited the help of his mother to attempt to contact the UC to send gifts and letters. KISOR made multiple attempts to contact the UC through the prison email system.

39. On or about January 26, 2023, KISOR contacted the UC again from the email account wrk1968@yahoo.com, the same email address he used in 2012 to communicate with the UC. At

this time, KISOR was incarcerated at the Alvis house. His actions were in violation of the aforementioned rules and subject to the listed consequences.

40. In an email KISOR sent in 2023, he attached a picture that the UC had sent to him in 2012 that she claimed was her then-14-year-old daughter. KISOR informed the UC that he had saved the image in his email storage. The UC explained that the daughter in the picture was now 24 years old, the younger daughter was now 14 years old, and she now had twin 8-year-old daughters. KISOR gave the UC his phone number of (614)753-6570 and repeatedly asked her to call him. He also repeatedly asked to send pictures of her daughters. Subsequently, KISOR began communicating with the UC via text message utilizing the phone number that he had given her. During their ongoing communications, the UC at various times presented herself as the mother and each of the four fictitious daughters that KISOR believed lived with her.

41. On or about February 17, 2023, KISOR sent text messages to the UC's phone believing that he was communicating with the UC's 24-year-old daughter, who was 14 years old at the time of their initial communications in 2012. In this conversation, KISOR asked if the 8-year-old twins' pubic hair is shaved and stated that he wanted "all the girls" to use sex toys on him and for him to use them on the girls.

42. On or about February 21, 2023, KISOR exchanged text messages with who he believed was the UC's 13-year-old daughter, who was 4 years old during the initial investigation. KISOR said, "I will be honored to be your stepfather and your first at sex," and asks if she wants KISOR to have sex with her. KISOR said that he "would like to do every hole that you have." KISOR went on to explain how he would be gentle with her "pussy" and asked if she would like to try a penis. Further, KISOR asked, "would you suck daddy's cock," and "would you swallow his cum," and tells her that he "would love to put my tongue in your pussy and butthole." KISOR asked if she wants kids and "what if I got you pregnant" saying, "would you want to have daddy's baby?". KISOR continued saying, "I can picture you fucking my cock while Ronnie [the eldest fictitious daughter] sits on my face while I eat her pussy." The UC the asked, "just me and Ronnie." KISOR responded saying, "all of you- twins also." Regarding the twins he asked, "would you like to see my cock in each of their little pussies or their buttholes?". The conversation continued with KISOR explaining how he wanted to have sex with all the girls and expressed that he wants them all to use sex toys on each other.

43. In another text message conversation on or about March 15, 2023, KISOR was communicating with the UC acting in the persona of the fictionalized girls' mother. KISOR stated "I really want to stick my cock in the twin's cunts." The UC then informed KISOR that he was communicating directly with one of the eight-year-old twins while the other twin sat with her. KISOR informed the girl "I would like to see you and olivia sucking my cock- and if you wanted me to, I would put my cock in your little pussies and assholes." The UC, continuing to act as one of the eight-year-old girls, asked if it will hurt and KISOR responded, "not if I tongue it enough." KISOR also asked the fictitious eight year old, "Did momma tell you that I want to pierce your little nipples," and stated that, "they look pretty for daddy and makes them super sensitive. You could cum just by me rubbing on your nipples." KISOR directly asked the child, "would you like to fuck daddy?". The UC responded asking, "does that mean we bounce up and down?". KISOR responded, "yes you can bounce up and down on daddy's cock." KISOR then went on to instruct the fictitious eight-year-old girls on how to stick their fists into their mother's vagina by "get all four fingers inside of momma, bring the thumb in towards the palm of your hand and once you do that, start pushing your fist into her cunt", and then to give her oral sex.

44. KISOR continued communicating or attempting to communicate with the UC, who was portraying the mother and the various fictitious daughters, through at least June of 2023, at which point the UC stopped responding. During those ongoing conversations, KISOR repeatedly suggested to the UC that she and her daughters visit him and stay at his home once he was released from the halfway house. KISOR specifically asked what he believed to be the 14-year-old daughter if she wanted to visit him in Ohio, and informed the mother that he was working to secure a home in the country where the children could run around naked.

45. On or about July 25, 2023, and in accordance with the Alvis House signed cell phone agreement and facilities rules, KISOR's phone, the SUBJECT DEVICE, was confiscated by Alvis House staff pending an investigation for violating the Alvis House rules regarding cell phone use. Pursuant to the agreement that KISOR signed, Alvis House staff conducted a preliminary review of the content that was immediately visible on the phone. During that review, staff observed web history on the phone indicating that it had been used to view videos on the website xhamster.com. From the screenshots of the phone that your affiant has reviewed,

xhamster.com appears to be a website offering free pornography videos and KISOR accessed a video on the website with a partial title of "Skinny Teen Aria."

46. Subsequent to the confiscation of his phone, the BOP placed KISOR in secured custody. KISOR was transferred to Franklin County Corrections Center II located at 2460 Jackson Pike, Columbus, Ohio 43223 on July 26, 2023. You affiant made contact with officials at the BOP and the Alvis House and obtained the SUBJECT DEVICE on or about August 29, 2023. It has been maintained in secure evidence storage at the Franklin County Sheriff's Office since it was obtained from the Alvis House.

VII. CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

47. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and are involved in exchanging child pornography with others and/or seeking sexual interactions with minors:

- a. Those who seek out, exchange, and/or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have while viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
- b. Those who seek out, exchange, and/or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Those who seek out, trade and/or collect child pornography sometimes maintain

hard copies of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections are often maintained for several years and are kept close by. More recently, however, those who have a sexual interest in children have more frequently been found to download, view, then delete child pornography on a cyclical and repetitive basis rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

- d. Those who seek out, trade and/or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and have been known to maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- e. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.


48. Based upon the conduct of individuals who have a sexual interest in minors as set forth in the above paragraphs, and the facts learned during the various investigations of William R. KISOR, namely, that KISOR has repeatedly sought to engage in sexual activities with minor females, that he has twice been convicted of federal child pornography crimes, and that he has recently been communicating about sexual activities with persons he believes to be minor females and has been accessing pornography websites on the internet, your affiant has reason to believe that KISOR has a sexual interest in minors and has viewed, distributed, or sought out visual depictions of minors engaged in sexually explicit conduct utilizing the SUBJECT

DEVICE. Furthermore, based on the information about KISOR's conduct contained herein, your affiant has reason to believe that KISOR has a sexual interest in minors and is an individual involved in exchanging child pornography, and all of the characteristics of such individuals that are described above may be applicable. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of distributing, receiving, and possessing child pornography and attempted coercion or enticement of a minor to engage in illegal sexual activity will be located in the SUBJECT DEVICE.

VIII. CONCLUSION

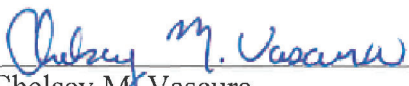
49. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that of violations of 18 U.S.C. §§ 2252, 2252A, and 2422(b) – the possession, receipt, and distribution of child pornography and the attempted coercion or enticement of a minor – have been committed, and evidence of those violations is located on the SUBJECT DEVICE, as more fully described in Attachment A, and for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252, 2252A, and 2422(b). Your affiant respectfully requests that the Court issue a search warrant authorizing the search of the SUBJECT DEVICE described in Attachment A and the seizure of the evidence described in Attachment B.

Respectfully submitted,



Joseph M Smith
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to before me this 14th day of September, 2023



Chelsey M Vascara
United States Magistrate Judge
Southern District of Ohio

ATTACHMENT A
Property to be Searched

The device to be searched is the following:

- i. Nokia N139DL bearing IMEI number 358712914117294 (**SUBJECT DEVICE**).

The **SUBJECT DEVICE** was seized from William R. Kisor on July 25, 2023, by Alvis House staff pursuant to the cell phone usage agreement that was signed by Kisor, permitting Alvis staff to search the **SUBJECT DEVICE** at any time with or without cause and to seize the **SUBJECT DEVICE** in the event that a violation of Alvis House rules is found on the device. The **SUBJECT DEVICE** was securely maintained by Alvis House staff until approximately August 29, 2023, when it was provided to Task Force Officer Joseph M. Smith of Homeland Security Investigations and the Internet Crimes Against Children Task Force. The **SUBJECT DEVICE** is currently held in the custody of the Franklin County Sheriff's Office Internet Crimes Against Children Property Room, located at 410 S. High Street, Columbus, Ohio 43215.

This warrant authorizes the forensic examination of **SUBJECT DEVICE** for the purpose of identifying and seizing the electronically stored information described in Attachment B.

ATTACHMENT B
List of Items to be Seized

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which has been used as the means of committing a criminal offense, namely 18 U.S.C. §§ 2252, 2252A, and 2422(b) – the distribution, receipt, and possession of child pornography in addition to coercion and enticement of a minor, those violations involving WILLIAM R KISOR including:

1. Any and all software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, e-mail or other application software.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages, other digital data files and web cache information) pertaining to sexual activity with minors or child pornography; communications regarding a sexual interest in minors; identification of individuals engaged in communications regarding sexual activity with minors or the exchange or accessing of child pornography; the existence of sites on the Internet that cater to those with a sexual interest in children or provide access to child pornography.

3. In any format and medium, any and all child pornography or child erotica.

4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning communications between William R. Kisor or any of his aliases or usernames and any other individuals related to the sexual abuse or exploitation of minor or the exchange, acquisition, or accessing of child pornography files.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the digital device, or by other means for the purpose of distributing or receiving child pornography.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by the internet, any child pornography.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

8. Notations of any password that may control access to an operating system or individual digital files.

9. Any and all records, documents, invoices, and materials, in any format or medium that concern any accounts with an Internet Service Provider or Electronic Communications Service.

10. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.

11. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography images or videos discovered.

12. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.